

IV. REMARKS

1. Claims 1-16 remain in the application. Claims 1-9, 11, and 14-16 have been amended.
2. Applicants respectfully submit that claims 1-16 are not anticipated by Dominguez et al. (US 2002/0194138, "Dominguez") under 35 USC 102(e).

Dominguez fails to disclose or suggest receiving a control message signal that includes a plurality of selective security protocols, as recited by claim 1.

Dominguez also does not disclose or suggest selecting one of the protocols received in the signal to protect information, also recited by claim 1.

Claim 1 recites "A device comprising...selection means connected to receive a control message signal from the second party said signal including a plurality of selectable security protocols and in response thereto to select one of the plurality of security protocols". The Examiner has indicated that this feature is disclosed in paragraphs [0069], [0070], [0076] and [0082], and has particularly pointed to paragraph [0076].

Paragraph [0076] of Dominguez discloses a merchant running a "merchant plug-in" querying the client device of a cardholder (i.e. the user purchasing goods) to determine whether the client device can support "distributed authentication". Lines 5-8 state that "the merchant plug-in will format and send a query, the QueryCardholderReq message, to the cardholder client device... to determine if a distributed PAS cardholder module is resident."

It is clearly stated that the device of claim 1 receives a control message signal including a plurality of selectable security protocols. The message received at the "cardholder client device" of Dominguez is the "QueryCardholderReq" message. This message is merely a query as to whether the cardholder client device "has distributed authentication capabilities". There is no mention that this message includes a plurality of selectable security protocols. Instead, this message is simply a request for information on the

capabilities of the cardholder client device, and provides no options for selection by the device. The applicants therefore submit that this "QueryCardholderReq" message does not include a plurality of selectable security protocols. Consequently, Dominguez therefore does not disclose that the cardholder client device comprises selection means to "select one of the plurality of security protocols".

In response to the "QueryCardholderReq" message, the cardholder client device in Dominguez sends a "QueryCardholderRes" message, which returns "distributed authentication options" to the merchant plug-in (paragraph [0076], line 10). These "distributed authentication options" are not analogous to the "plurality of selectable security protocols" for the reasons stated below. Nevertheless, it is clear that any action taken as a result of these "distributed authentication options" is made at the merchant plug-in, and not at the device as recited in claim 1. Therefore, the applicants submit that Dominguez does not disclose the device selecting one of the plurality of security protocols. In any case, there is no explicit disclosure of the merchant plug-in performing a "selection" from the distributed authentication options.

The applicants further assert that, in any case, "distributed authentication options" are not the same as a plurality of selectable security protocols. Paragraph [0050] states that "Cardholder authentication information includes information such as business identification, country code, card account number, card expiration date, cardholder name, issuer-specific authentication data..., and other information such as billing address, shipping address, social security number, telephone number, account balance, transaction history, and driver licence number". In contrast, claim 1 states that "information transferred subsequently between the device and second party is protected using the selected security protocol". It is therefore clear that there is a significant difference between "authentication options" which is specific information for authenticating a user, and a security protocol, which is used to protect information transmitted across a communication link. The term "protocol" is well known to the skilled person, and the skilled person would not equate a security protocol to be the same as authentication options.

Independent claim 14 recites the feature of “selection means for selecting one of a plurality of security protocols and being connected to communicate said selection to said second party”. Independent claim 15 recites “selection means for selecting a SET security protocol and being connected to communicate said selection to said second party” and independent claim 16 recites “selection means for selecting a EMV security protocol and being connected to communicate said selection to said second party”. As stated previously, Dominguez does not mention a device comprising a selection means for selecting a security protocol, and therefore the applicants submit that independent claims 14, 15 and 16 can also be distinguished over Dominguez for the same reasons as outlined above.

At least for these reasons, Applicants submit that Dominguez does not anticipate independent claims 1 and 14-16 and dependent claims 2-13.

3. Applicants respectfully submit that claims 1, 2, 5, 8-10, 11, and 13 are not anticipated by Williams et al. (US 5,963,924, “Williams”) under 35 USC 102(e).

Williams fails to disclose or suggest receiving a control message signal that includes a plurality of selectable security protocols, and selecting one of the protocols to protect information, as recited by claim 1.

The Examiner has pointed to column 16, line 52-56 of Williams, which states that “once the consumer authorizes the payment, the payment protocol is decided by PayWindow based on the merchant’s Payment Protocol Preferences and the consumer selected payment instrument”. The Examiner is alleging that this statement anticipates the “selection means connected to receive a control message signal from the second party said signal including a plurality of selectable security protocols and in response thereto to select one of the plurality of security protocols” recited in claim 1. The applicants assert that the Examiner is using knowledge of the present invention and hindsight to read features into the statement in Williams.

The applicants submit that nowhere does Williams disclose or suggest that a control message signal is sent from merchant to the consumer, which includes a plurality of

selectable security protocols. The Examiner states that "the Pay Window system contains the necessary programming to interface the wishes of the user and the availabilities of the system, including the necessary security protocols". Therefore, the Examiner seems to be saying that Williams does not explicitly disclose the sending of the control message, but that it is implicit. The applicants strongly disagree. There is simply nothing in Williams to suggest transmitting "a plurality of selectable security protocols" to the user. The payment protocol is explicitly decided by PayWindow based on the merchant's Payment Protocol Preferences and the consumer selected payment instrument. There is nothing that suggests transmitting protocols to a user for selection. In addition, there is nothing that suggests transmitting a plurality of protocols at all. For example, it is just as likely that the merchant may only support a single security protocol.

In addition, claim 1 recites that in response to receiving the control message, the selection means selects one of the plurality of security protocols. There is no indication or disclosure in Williams that the selection of security protocols would be performed in response receiving any control message that may (implicitly) be sent. Any communication of merchant preferences could equally be sent a long time in advance of any selection and stored. Any selection from these preferences would therefore not be in response to receiving the message.

It is therefore clear that Williams does not disclose "selection means connected to receive a control message signal from the second party said signal including a plurality of selectable security protocols and in response thereto to select one of the plurality of security protocols". The applicants therefore submit that claim 1 is not anticipated by Williams.

At least for these reasons, Applicants submit that Williams does not anticipate independent claim 1 and dependent claims 2, 5, 8-10, 11 and 13.

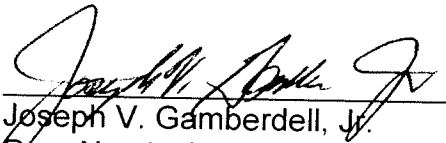
For all of the foregoing reasons, it is respectfully submitted that all of the claims now present in the application are clearly novel and patentable over the prior art of record,

and are in proper form for allowance. Accordingly, favorable reconsideration and allowance is respectfully requested. Should any unresolved issues remain, the Examiner is invited to call Applicants' attorney at the telephone number indicated below.

Please charge Deposit Account No. 16-1350 \$450.00 for a two (2) month extension of time.

The Commissioner is hereby authorized to charge payment for any fees associated with this communication or credit any over payment to Deposit Account No. 16-1350.

Respectfully submitted,


Joseph V. Gamberdell, Jr.
Reg. No. 44,695

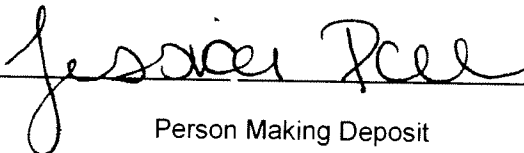
31 October 2006
Date

Perman & Green, LLP
425 Post Road
Fairfield, CT 06824
(203) 259-1800
Customer No.: 2512

CERTIFICATE OF ELECTRONIC FILING

I hereby certify that this correspondence is being deposited transmitted electronically, on the date indicated below, addressed to the Mail Stop AMENDMENT, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

Date: 10.31.2006

Signature: 
Person Making Deposit